Statement
of
Stan O. Barber
Vice President of Engineering Operations,
Verio, Inc.

Before the
Committee on Government Reform
U.S. House of Representatives

June 29, 2005

Mr. Chairman and Members of the Committee, it is a distinct honor to speak to you today about the Next Generation Internet and the Transition to Internet Protocol version 6. My name is Stan Barber and I am the Vice President of Engineering Operations of Verio, Inc. Verio is one of the world's leading Internet service providers and one of several so-called Tier 1 Internet backbone providers, the networks with sufficient reach, scale and traffic to afford their customers and customers of other, interconnecting networks, including US government users, global connectivity. Verio is based in Englewood, Colorado and is a subsidiary of NTT Communications Corporation and an affiliate of NTT America, Inc. The Committee is to be congratulated for its focus on the next generation of Internet services. We all recognize that the Internet has become in a few short years a fundamental aspect of our economy and essential to the productivity of business and delivery of government services.

To some, the term "next generation" suggests speculation about future technological developments, and wide expanses of time and opportunities to identify and address issues. However, we live on Internet time, and, "next generation" in that context means "Now."

Indeed, the next generation of the Internet-- IPv6-- was defined as an open source, non-proprietary protocol in the 1990s and has already found its place extensively in major computer operating systems such as Windows XP and Linux and in many public and private networks around the world. I believe that my company, Verio, is the world's most experienced commercial IPv6 service provider and operates the most extensive commercial IPv6 network. Most networks today still operate in the older IP version 4 protocol, but the transition to the later technology is essential and inevitable because of the inherent advantages built into IPv6.

IPv4 does not today provide for sufficient addresses to accommodate efficiently connectivity to all potential users worldwide. IPv6, on the other hand, increases the number of directly addressable nodes exponentially. While security for IPv4 is provided where practical as a "patch", using overlay systems, IPv6 builds in high level security protections, such as secure remote node authentication and encryption, directly into the network layer, assuring more reliable and ubiquitous protection. IPv6 generally increases flexibility and functionality with additional benefits, such as more efficient routing of traffic and more effective usage with wireless devices. The result is lower costs and improved services, like end-to-end communications and communications with devices other than PCs, something we call m2m-x communications. That is why Internet equipment manufacturers and the leading software providers, service providers and private network operators have started to transition from v4 to v6, and those that have not as yet, will inevitably find that flexibility, efficiency and security requires the conversion.

Other countries are ahead of the United States in this transition. This does not reflect any genuine technological advantage over the US. Indeed, it may be said that the US continues to lead the rest of the world in Internet and related technology. Other countries have advanced to IPv6 primarily because of an initial lag in Internet development. Consequently, they have been more keenly focused on the need to address the shortage of Internet addresses and less extensive legacy networks in need of transition. For example:

- The European Commission created a task force to design a plan of action for development, testing and deployment of IPv6 in 2001. The task force is coordinating efforts in individual member counties and regions and seeking cooperation with other countries.
- The Chinese government has established an IPv6 network linking major universities. The government is also funding a plan to develop a more extensive IPv6 infrastructure.
- Taiwan is also developing a national information infrastructure built on IPv6.
- India has established the IPv6 Forum to coordinate development and implementation of IPv6.
- In Japan, the home of our parent company, the government's e-Japan Strategy has been promoting the transition to IPv6 Internet. In addition, an e-Government Creation Plan facilitates the procurement of IPv6-capable devices. In the commercial sector, the IPv6 Promotion Council helps address issues related to the transition.

I have described these initiatives in other countries not to advocate any US government mandate or funding of transition to IPv6 in the private sector, but to note the clear recognition by policymakers abroad of the potential of IPv6. This Committee is showing its characteristic leadership in bringing to the attention of the public the need for an effective transition from legacy Internet technologies in government and more generally. The report of the Government Accountability Office requested by this Committee demonstrates a deep understanding of the issues raised by this technological transition. The GAO offers solid recommendations to save government money and to protect against security threats.

In addition to GAO's comments, it is also useful to recognize that the transition to IPv6 need not be disruptive or costly. Verio and NTT Communications employ the so-called "dual stack" transition strategy globally in which we run simultaneous IPv4 and IPv6 systems. Use of the IPv6 system is selected where a peer has that capability; the legacy protocol is employed where the peer cannot be reached in IPv6. Thus, the transition is transparent to users and existing software and equipment. Software and equipment that does not accommodate IPv6 can be updated in conjunction with normal upgrades or as specially designated by management. The key point is that, as recognized by the GAO report, government and private sector management should at least be surveying their essential IT operations to accommodate the inevitable transition.

In this regard, the GAO and this Committee are also to be congratulated for highlighting an extremely important issue of security related to on-going employment of legacy IPv4

networks in the transition to IPv6. As I have indicated, some operating systems, including such ubiquitous systems as Windows XP, Apple's OS X, Linux and Unix-based systems, already accommodate IPv6, although they are used primarily in this country in conjunction with the legacy network protocol. Similarly, many software applications today accommodate IPv6. Not all IT managers are aware of the potential of a grave security threat to their systems by allowing unauthorized parties access to software using "ghost" IPv6 addresses unrecognized by their systems because they are buried within IPv4 addressed packets. Or, if they are aware of the threat, they do not have the budgets and other resources to address the problem. Even as government agencies and the private sector transition, as they must, from the legacy platform to IPv6, they must be vigilant in adapting firewalls and other equipment and software to prevent unauthorized parties from using IPv6 capabilities accessed covertly over existing IPv4 networks.

Mr. Chairman, I thank you again for the opportunity to address this Committee about these critical issues of technological development and implementation, and for your leadership in identifying and making the public aware of these important matters. Verio stands ready to continue to assist further the Committee in any way we can.